



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/698,128 | 10/31/2003 | Simon C. Chu | RPS920030115US3 | 8930 |

7590 03/22/2006

IBM Corporation
Intellectual Property Law Dept. 9CCA/B002
P.O. Box 12195
Res. Tri. Park, NC 27709

EXAMINER

STOYNOV, STEFAN

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2116

DATE MAILED: 03/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | | |
|------------------------------|--------------------------------------|-----------------------------------|--|
| Office Action Summary | Application No. 10/698,128 | Applicant(s) CHU ET AL. | |
| | Examiner Stefan Stojnov | Art Unit 2116 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date: _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date: _____ | 6) <input type="checkbox"/> Other: _____ |

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-8 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-24 of copending Application No. 10/674,776. Although the conflicting claims are not identical, they are not patentably distinct from each other because the limitations in claims 1-8 are disclosed in claims 1-24 of copending Application No. 10/674,776.

Claims 1-8 are nearly identical to claims 1-24 of copending Application No. 10/674,776 except that claims 1-8 in the current application recite "a service for managing a network boot of a client computer", whereas claims 1-24 of copending Application No. 10/674,776 recite "a method, a system, and a computer program product for managing a network boot of a client computer". The referred claims

encompass any one of “a service, a method, a system, and a computer program product for managing a network boot of a client computer”.

Claim 1 is provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1, 2, 6, 7, 11, and 12 of copending Application No. 10/675,624. Although the conflicting claims are not identical, they are not patentably distinct from each other because the limitations in claim 1 are disclosed in claims 1, 2, 6, 7, 11, and 12 of copending Application No. 10/675,624.

Claim 1 is nearly identical to claims 1, 2, 6, 7, 11, and 12 of copending Application No. 10/675,624 except that claim 1 in the current application recites “request for a boot program” and “boot program servers”, whereas claims 1, 2, 6, 7, 11, and 12 of copending Application No. 10/675,624 recite “request for a configuration parameter” and “configuration servers”. A “request for a boot program” is a “request for configuration parameter” because the boot program provides configuration parameters.

Claims 1 and 6 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1 and 2 of copending Application No. 10/698,207. Although the conflicting claims are not identical, they are not patentably distinct from each other because the limitations in claims 1 and 6 are disclosed in claims 1 and 2 of copending Application No. 10/698,207.

Claims 1 and 6 are nearly identical to claims 1 and 2 of copending Application No. 10/698,207 except that claims 1 and 6 in the current application recite “request for a boot program” and “boot program servers”, whereas claims 1 and 2 of copending Application No. 10/698,207 recite “request for a configuration parameter” and

"configuration servers". A "request for a boot program" is a "request for configuration parameter" because the boot program provides configuration parameters.

These are provisional obviousness-type double patenting rejections because the conflicting claims have not in fact been patented.

Claim Objections

Claim 1 is objected to because of the following informalities:

In line 1, claim 1 refers to "A service", but recites "the method" at the end of the line.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4 and 5 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 4 recites the limitation "the designated administrator" in line 1.

Claim 5 recites the limitation "the blade server" in lines 1 and 2.

There is insufficient antecedent basis for these limitations in the claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and

Art Unit: 2116

the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zimmer et al., US Patent Appl. Pub. Num. 2004/0193867, in view of Schell et al., US Patent Num. 6,314,520.

Re claim 1, Zimmer discloses a service for managing a network boot of a client computer, the method comprising:

broadcasting a request for a boot program from the client computer to a network of boot program servers (paragraph 0020, lines 4-8, FIG. 2, 202, paragraph 0021, lines 5-10);

receiving a response to the request for the boot program at the client computer, the response being from a responding boot program server on the network of boot servers (paragraph 0025, lines 1-3, FIG. 2, 204);

requesting and downloading onto the client computer a boot program from the responding boot program server (paragraph 0030, line 1, paragraph 0031, lines 1-4, FIG. 2, 208 and 210);

In addition, Zimmer discloses the interface card also being coupled to a hyper-secure remote service network.

[Zimmer does not specifically state the interface service card also being coupled to a hyper-secure remote service network. However, Zimmer discloses a network interface card (NIC) coupled to the remote system (remote server) via a network (e.g. LAN, WAN, or Internet) (paragraph 0048, lines 9-14, FIG. 4). Zimmer further discloses selectively providing remote boot options based on security requirements of the client machine (paragraph 0026, lines 1-9). Thus, a network security policy is established within the corporate network (paragraph 0023, lines 6-8) including the client's machine coupled to the remote server (via a NIC), and thus Zimmer discloses the interface service card also being coupled to a hyper-secure remote service network.]

Zimmer fails to disclose storing a list of trusted boot program servers in an interface service card coupled to a client computer, comparing an identity of the responding boot program server with the list of trusted boot program servers, and upon verifying that the responding boot program server is on the list of trusted boot program servers,

requesting and downloading onto the client computer a boot program from the responding boot program server (this step was addressed by Zimmer as indicated above and was added here for clarity).

Schell teaches a networked client/server computer system configured to establish a trusted workstation (column 1, lines 20-22). Schell further teaches each workstation having a network interface card (NIC), which establishes a trusted

connection between the workstation and the server (column 3, lines 62-65, FIG. 1, 14, 20) through which the workstation communicates with the server over the computer network (column 4, lines 5-7, FIG. 1, 12, 14). In addition, Schell further teaches the NIC card containing a trusted computing base (TCB) extensions that provide for securely booting the workstation, the "TBC extensions" referring to extensions of the server's TCB that operate as part of the workstation's network trusted computing base (column 2, lines 3-11) (i.e. database of trusted servers contained on the NIC). Schell also teaches an address confirmation circuit, wherein upon receipt of a packet, the source address of the received packet is compared for verification that it was sent from an authorized server (i.e. identity verification) (column 2, lines 30-35, column 3, lines 6-11, column 4, line 64- column 5, line 2, column 5, lines 13-22). In Schell, the pre-boot modules are downloaded to the workstation from known trusted servers only (column 2, lines 50-54, column 3, lines 45-49) after meeting the identity verification criteria. Thus, the security of the information stored on a client/server is ensured (column 1, lines 56-59).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use the system and method of storing a trusted computing base (TCB) extension corresponding to trusted boot servers within a NIC used for communication over a network, the process or identity comparison and verification of the received network packets, and based upon that comparison downloading pre-boot modules to the client machine from trusted servers, as suggested by Schell with the method, system, and computer program product disclosed by Zimmer in order to

implement storing a list of trusted boot program servers in an interface service card coupled to a client computer on a network, comparing an identity of the responding boot program server with the list of trusted boot program servers, and upon verifying that the responding boot program server is on the list of trusted boot program servers, requesting and downloading onto the client computer a boot program from the responding boot program server. One of ordinary skill in the art would be motivated to do so in order to ensure security of the information being downloaded to the client computer.

Re claim 2, Schell further teaches the service, further comprising:

upon determining that the responding boot program server is not on the list of the trusted boot program servers, blocking the requesting of the boot program from the responding boot program server (column 5, lines 20-22).

Re claim 3, Zimmer further discloses the service as per claim 2, further comprising:

upon determining that the responding boot program server is not on the list of trusted boot program servers, generating an alert to a designated administrator of a presence of an unauthorized boot program server on the network of boot program servers (paragraph 0044, lines 12-15).

Re claim 4, Zimmer discloses the hyper-secure network as per claim 1. In addition, Schell further teaches the service, wherein the designated administrator communicates with the client computer via the hyper-secure remote service network.

[Schell does not specifically state wherein the designated administrator communicates with the client computer via the hyper-secure remote service network. However, Schell teaches using usernames and passwords in the process of verification for the trusted server (column 6, line 21- column 7, line 53). Thus, these usernames and passwords are assigned and maintained (i.e. by an administrator), and thus Schell teaches, wherein the designated administrator communicates with the client computer via the hyper-secure remote service network.]

Re claim 5, Zimmer further discloses the service as per claim 4, wherein the comparing step is performed by configuring the blade server to perform Layer 3 packet filtering to identify Pre-boot Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open System Interconnection (OSI) model (paragraph 0014, lines 3-6, paragraph 0037, lines 1-10, paragraph 0038, lines 1-6).

Re claim 6, Schell further teaches the service, further comprising:
upon determining that the responding boot program server is not on the list of trusted boot program servers, downloading a boot program from a known trusted boot server in a secure local area network LAN.

[Schell does not specifically state upon determining that the responding boot program server is not on the list of trusted boot program servers, downloading a boot program from a known trusted boot server in a secure local area network LAN. However, Schell teaches discarding the received network packets transmitted by an unauthorized server (column 5, lines 20-22). Thus, it is determined that an untrusted

server sent the packets and no download is initiated towards the client computer (i.e. determining that the responding boot program server is not on the list of trusted boot program servers). Only when the network packets are verified to be from a trusted server, the download is permitted over the LAN (column 3, lines 53-55, column 5, lines 13-20) (i.e. downloading a boot program from a known trusted boot server in a secure local area network LAN).]

Re claim 7, Zimmer and Schell disclose all claim limitations as per claim 1.

Zimmer and Schell do not specifically state wherein the client computer is a server blade. However, Zimmer discloses the client computer not limited to a personal computer, network workstation, etc. (paragraph 0015, lines 1-2) in the network environment. In addition, the examiner takes an Official Notice for the client computer being a server blade. It is well known in the art for aggregating network modules (clients) as blades in a blade-server architecture in order to provide system scalability. Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the client computer being a server blade. One of ordinary skill in the art would be motivated to do so in order to achieve system scalability for plurality of clients.

Re claim 8, Zimmer and Schell further disclose the service as per claim 7, further comprising:

managing different types of boot program servers available to the server blade by maintaining, in an information technology services organization logically oriented between the different types of boot program servers and the server blade (Zimmer,

Art Unit: 2116

paragraph 0022, lines 1-20), a permission list of boot program servers authorized for each server blade in a server blade chassis (Schell, column 2, lines 3-11).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stefan Stoynov whose telephone number is (571) 272-4236. The examiner can normally be reached on 8:00AM-4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lynne Browne can be reached on (571) 272-3670. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SS


LYNNE H. BROWNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100